

Docket No.: 60188-648

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of : Customer Number: 20277
: :
Makoto FUJIWARA, et al. : Confirmation Number:
: :
Serial No.: : Group Art Unit:
: :
Filed: September 04, 2003 : Examiner:
: :
For: SEMICONDUCTOR DEVICE INCLUDING ENCRYPTION SECTION,
SEMICONDUCTOR DEVICE INCLUDING EXTERNAL INTERFACE, AND
CONTENT REPRODUCTION METHOD

**CLAIM OF PRIORITY AND
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT**

Mail Stop
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 35 U.S.C. 119, Applicants hereby claim the priority of:

Japanese Patent Application No. 2002-258481, filed September 4, 2002

cited in the Declaration of the present application. A Certified copy is submitted herewith.

Respectfully submitted,


MCDERMOTT, WILL & EMERY

Michael E. Fogarty
Registration No. 36,139

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 MEF:prg
Facsimile: (202) 756-8087
Date: September 4, 2003

日 本 国 特 許 庁

JAPAN PATENT OFFICE

001800210
Fujiwara et al.
Sept-4, 2003

McDermott, Will & Emery

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年 9月 4日

出 願 番 号

Application Number:

特願2002-258481

[ST.10/C]:

[JP 2002-258481]

出 願 人

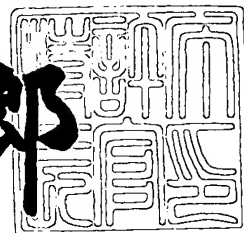
Applicant(s):

松下電器産業株式会社

2003年 4月25日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田信一郎



出証番号 出証特2003-3030830

【書類名】 特許願

【整理番号】 5037540107

【提出日】 平成14年 9月 4日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 15/00

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式
会社内

【氏名】 藤原 睦

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式
会社内

【氏名】 根本 祐輔

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式
会社内

【氏名】 安井 純一

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式
会社内

【氏名】 前田 卓治

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式
会社内

【氏名】 伊藤 孝幸

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式
会社内

【氏名】 山田 泰司

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 井上 信治

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100077931

【弁理士】

【氏名又は名称】 前田 弘

【選任した代理人】

【識別番号】 100094134

【弁理士】

【氏名又は名称】 小山 廣毅

【選任した代理人】

【識別番号】 100110939

【弁理士】

【氏名又は名称】 竹内 宏

【選任した代理人】

【識別番号】 100110940

【弁理士】

【氏名又は名称】 嶋田 高久

【選任した代理人】

【識別番号】 100113262

【弁理士】

【氏名又は名称】 竹内 祐二

【選任した代理人】

【識別番号】 100115059

【弁理士】

【氏名又は名称】 今江 克実

【選任した代理人】

【識別番号】 100115510

【弁理士】

【氏名又は名称】 手島 勝

【選任した代理人】

【識別番号】 100115691

【弁理士】

【氏名又は名称】 藤田 篤史

【手数料の表示】

【予納台帳番号】 014409

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0006010

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗号化部を有する半導体装置、外部インターフェースを有する半導体装置、およびコンテンツ再生方法

【特許請求の範囲】

【請求項 1】 プログラムの暗号化および復号化のうち少なくともいずれか一方を行う暗号化部を備え、

前記暗号化部は、

プログラムの暗号化処理または復号化処理を含む複数のシーケンスを実行可能な暗号化演算部と、

前記暗号化演算部が実行可能な各シーケンスについて、実行の諾否を判断し、実行が許されないと判断したシーケンスについて、前記暗号化演算部の動作を禁止する暗号化制御部とを備えたものであることを特徴とする半導体装置。

【請求項 2】 請求項 1 において、

前記複数のシーケンスは、鍵の暗号化処理または復号化処理を含むものであることを特徴とする半導体装置。

【請求項 3】 請求項 1 において、

前記暗号化制御部は、

モード ID を格納するためのモード ID 格納レジスタを備え、かつ、

前記モード ID 格納レジスタに格納されたモード ID の値に基づいて、各シーケンスの実行の諾否を判断するものであることを特徴とする半導体装置。

【請求項 4】 請求項 3 において、

前記暗号化制御部は、

前記各シーケンスに対応して設けられ、その発行回数を格納するためのレジスタを備え、

前記モード ID の値に加えて、前記レジスタに格納された前記各シーケンスの発行回数を加味して、各シーケンスの実行の諾否を判断するものであることを特徴とする半導体装置。

【請求項 5】 請求項 3 において、

書き換え不可領域を有するセキュアメモリを備え、前記書き換え不可領域には、前記モード I D が記憶されており、

前記モード I D 格納レジスタは、当該半導体装置の起動時にのみ書き込み可能であり、かつ、起動時に、前記セキュアメモリの前記書き換え不可領域から読み出された前記モード I D が書き込まれることを特徴とする半導体装置。

【請求項 6】 請求項 5 において、

ブートプログラムを記憶するブート R O M を備え、

前記モード I D 格納レジスタへの前記モード I D の書き込みは、前記ブート R O M に記憶されたブートプログラムによって、実行することを特徴とする半導体装置。

【請求項 7】 請求項 3 において、

当該半導体装置が初めて起動されたか否かを表す実装モードフラグを記憶するセキュアメモリを備え、

前記暗号化制御部は、

前記モード I D の値に加えて、前記実装モードフラグを参照して、各シーケンスの実行の諾否を判断するものであることを特徴とする半導体装置。

【請求項 8】 請求項 1 において、

前記複数のシーケンスの少なくとも 1 つについて、これに対応したブートプログラムを記憶するブート R O M を備え、

前記暗号化演算部は、前記ブート R O M に記憶されたブートプログラムを実行することによって、シーケンスを実行するものであることを特徴とする半導体装置。

【請求項 9】 請求項 1 において、

前記暗号化演算部および暗号化制御部が有するレジスタについて、当該半導体装置外部からのアクセスができないように制御する手段を備えたことを特徴とする半導体装置。

【請求項 1 0】 外部メモリとの間で、プログラムやデータの入出力を行うための外部インターフェースを備え、

前記外部インターフェースは、

プログラムの入出力を行うプログラム処理部と、

データの入出力を行うデータ処理部とを備え、

前記プログラム処理部と前記データ処理部とは、別個独立に、構成されていることを特徴とする半導体装置。

【請求項 1 1】 請求項 1 0 において、

前記プログラム処理部は、

プログラムをそのまま入出力するスルー部と、

前記外部メモリに記憶された暗号化プログラムを受け、これを平文プログラムに復号して、当該半導体装置内部に供給するプログラム復号用暗号エンジンとを備えたものである

ことを特徴とする半導体装置。

【請求項 1 2】 請求項 1 1 において、

前記スルー部は、実行用スルー部と、暗号化用スルー部とを備えており、

前記実行用スルー部を介して入力されたプログラムは、当該半導体装置において実行される一方、前記暗号化用スルー部を介して入力されたプログラムは、暗号化部に供給され、暗号化される

ことを特徴とする半導体装置。

【請求項 1 3】 請求項 1 2 において、

前記外部メモリにおける各領域と、アドレスとの対応関係を表すアドレス管理情報を格納するアドレス区分格納レジスタを備え、

前記外部メモリにアクセスしてプログラムを読み込むとき、前記アドレス管理情報を参照して、前記暗号化用スルー部、前記実行用スルー部および前記プログラム復号用暗号エンジンのいずれを有効にするかを、決定する

ことを特徴とする半導体装置。

【請求項 1 4】 請求項 1 3 において、

前記アドレス区分格納レジスタは、当該半導体装置の起動時にのみ書き込み可

能である

ことを特徴とする半導体装置。

【請求項 1 5】 請求項 1 4 において、

書き換え不可領域を有するセキュアメモリを備え、前記書き換え不可領域には、前記アドレス管理情報が記憶されており、

前記アドレス区分格納レジスタは、当該半導体装置の起動時に、前記セキュアメモリの前記書き換え不可領域から読み出された前記アドレス管理情報が書き込まれる

ことを特徴とする半導体装置。

【請求項 1 6】 請求項 1 3 において、

モード I D を格納するためのモード I D 格納レジスタを有するモードシーケンサを備え、

前記モード I D 格納レジスタに格納されたモード I D の値を加味して、前記暗号化用スルー部、前記実行用スルー部および前記プログラム復号用暗号エンジンのいずれを有効にするかを、決定する

ことを特徴とする半導体装置。

【請求項 1 7】 請求項 1 6 において、

前記モードシーケンサは、ジャンパ値判定部を備え、

前記ジャンパ値判定部によって判定されたジャンパ値を加味して、前記暗号化用スルー部、前記実行用スルー部および前記プログラム復号用暗号エンジンのいずれを有効にするかを、決定する

ことを特徴とする半導体装置。

【請求項 1 8】 請求項 1 0 において、

前記データ処理部は、

データをそのまま入出力するスルー部と、

データの入出力の際に、暗号または復号を行うデータ暗復号用暗号エンジンとを備えたものである

ことを特徴とする半導体装置。

【請求項 1 9】 外部メモリの再生不可領域に格納された原コンテンツを、

L S I に取り込むステップと、

前記 L S I において、内部メモリに格納された固有 I D を用いて、データ固有鍵を生成するステップと、

前記 L S I において、前記原コンテンツを、前記データ固有鍵を用いて暗号化するステップと、

暗号化されたコンテンツを、前記外部メモリの再生可能領域に格納するステップと、

前記再生可能領域に格納された前記暗号化されたコンテンツを、前記 L S I に取り込み、前記データ固有鍵を用いて復号化して再生するステップとを備えたことを特徴とするコンテンツ再生方法。

【請求項 2 0】 請求項 1 9 において、

前記原コンテンツは、データ共有鍵で暗号化されたものであり、

前記原コンテンツを、前記データ固有鍵を用いて暗号化する前に、内部メモリに格納された前記データ共有鍵を用いて、復号化することを特徴とするコンテンツ再生方法。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、鍵実装システムに用いられる L S I のような半導体装置において、セキュリティを向上させる技術に属する。

【 0 0 0 2 】

【従来の技術】

本願と同一の出願人による特願 2 0 0 1 - 2 8 6 8 8 1 では、鍵実装システムにおいて、鍵の機密性および秘匿性を、従来よりも向上させる技術が示されている。

【 0 0 0 3 】

しかし、かかる先行技術は、文献公知発明に係るものではないため、記載すべき先行技術文献情報はない。

【 0 0 0 4 】

【発明が解決しようとする課題】

本発明は、セキュリティレベルの高い半導体装置を提供することを課題とする。また、セキュリティレベルの高いコンテンツ再生方法を提供することを課題とする。

【0005】

【課題を解決するための手段】

前記の課題を解決するために、本発明が講じた解決手段は、半導体装置として、プログラムの暗号化および復号化のうち少なくともいずれか一方を行う暗号化部を備え、前記暗号化部は、プログラムの暗号化処理または復号化処理を含む複数のシーケンスを実行可能な暗号化演算部と、前記暗号化演算部が実行可能な各シーケンスについて、実行の諾否を判断し、実行が許されないと判断したシーケンスについて、前記暗号化演算部の動作を禁止する暗号化制御部とを備えたものである。

【0006】

本発明によると、暗号化部において、暗号化制御部が、暗号化演算部が実行可能な各シーケンスのうち、実行が許されないと判断したシーケンスについて、暗号化演算部の動作を禁止する。すなわち、実行が許されると暗号化制御部によって判断されたシーケンスのみが、暗号化演算部によって実行される。このため、シーケンスの不正実行を未然に防止することができ、セキュリティレベルが向上する。

【0007】

そして、前記本発明に係る半導体装置における複数のシーケンスは、鍵の暗号化処理または復号化処理を含むのが好ましい。

【0008】

また、前記本発明に係る半導体装置における暗号化制御部は、モードIDを格納するためのモードID格納レジスタを備え、かつ、前記モードID格納レジスタに格納されたモードIDの値に基づいて、各シーケンスの実行の諾否を判断するのが好ましい。

【0009】

そして、前記暗号化制御部は、前記各シーケンスに対応して設けられ、その発行回数を格納するためのレジスタを備え、前記モードIDの値に加えて、前記レジスタに格納された前記各シーケンスの発行回数を加味して、各シーケンスの実行の諾否を判断するのが好ましい。

【0010】

また、書き換え不可領域を有するセキュアメモリを備え、前記書き換え不可領域には、前記モードIDが記憶されており、前記モードID格納レジスタは、当該半導体装置の起動時にのみ書き込み可能であり、かつ、起動時に、前記セキュアメモリの前記書き換え不可領域から読み出された前記モードIDが書き込まれるのが好ましい。さらに、ブートプログラムを記憶するブートROMを備え、前記モードID格納レジスタへの前記モードIDの書き込みは、前記ブートROMに記憶されたブートプログラムによって実行するのが好ましい。

【0011】

また、当該半導体装置が初めて起動されたか否かを表す実装モードフラグを記憶するセキュアメモリを備え、前記暗号化制御部は、前記モードIDの値に加えて、前記実装モードフラグを参照して、各シーケンスの実行の諾否を判断するのが好ましい。

【0012】

また、前記本発明に係る半導体装置は、前記複数のシーケンスの少なくとも1つについて、これに対応したブートプログラムを記憶するブートROMを備え、前記暗号化演算部は、前記ブートROMに記憶されたブートプログラムを実行することによってシーケンスを実行するのが好ましい。

【0013】

また、前記本発明に係る半導体装置は、前記暗号化演算部および暗号化制御部が有するレジスタについて、当該半導体装置外部からのアクセスができないように制御する手段を備えているのが好ましい。

【0014】

また、本発明は、半導体装置として、外部メモリとの間で、プログラムやデータの入出力を行うための外部インターフェースを備え、前記外部インターフェー

スは、プログラムの入出力を行うプログラム処理部と、データの入出力を行うデータ処理部とを備え、前記プログラム処理部と前記データ処理部とは、別個独立に、構成されているものである。

【0015】

本発明によると、外部インターフェースにおいて、プログラム処理部とデータ処理部とが、別個独立に、構成されている。このため、プログラムが不正実行されるリスクが分散されることになり、セキュリティレベルが向上する。

【0016】

そして、前記本発明に係る半導体装置におけるプログラム処理部は、プログラムをそのまま入出力するスルー部と、前記外部メモリに記憶された暗号化プログラムを受け、これを平文プログラムに復号して、当該半導体装置内部に供給するプログラム復号用暗号エンジンとを備えているのが好ましい。

【0017】

さらに、前記スルー部は、実行用スルー部と、暗号化用スルー部とを備えており、前記実行用スルー部を介して入力されたプログラムは、当該半導体装置において実行される一方、前記暗号化用スルー部を介して入力されたプログラムは、暗号化部に供給され、暗号化されるのが好ましい。

【0018】

さらに、前記外部メモリにおける各領域と、アドレスとの対応関係を表すアドレス管理情報を格納するアドレス区分格納レジスタを備え、前記外部メモリにアクセスしてプログラムを読み込むとき、前記アドレス管理情報を参照して、前記暗号化用スルー部、前記実行用スルー部および前記プログラム復号用暗号エンジンのいずれを有効にするかを、決定するのが好ましい。

【0019】

さらに、前記アドレス区分格納レジスタは、当該半導体装置の起動時にのみ書き込み可能であるのが好ましい。

【0020】

さらに、書き換え不可領域を有するセキュアメモリを備え、前記書き換え不可領域には、前記アドレス管理情報が記憶されており、前記アドレス区分格納レジ

スタは、当該半導体装置の起動時に、前記セキュアメモリの前記書き換え不可領域から読み出された前記アドレス管理情報が書き込まれるのが好ましい。

【0021】

または、モードIDを格納するためのモードID格納レジスタを有するモードシーケンサを備え、前記モードID格納レジスタに格納されたモードIDの値を加味して、前記暗号化用スルー部、前記実行用スルー部および前記プログラム復号用暗号エンジンのいずれを有効にするかを、決定するのが好ましい。

【0022】

さらに、前記モードシーケンサは、ジャンパ値判定部を備え、前記ジャンパ値判定部によって判定されたジャンパ値を加味して、前記暗号化用スルー部、前記実行用スルー部および前記プログラム復号用暗号エンジンのいずれを有効にするかを決定するのが好ましい。

【0023】

また、前記本発明に係る半導体装置におけるデータ処理部は、データをそのまま入出力するスルー部と、データの入出力の際に、暗号または復号を行うデータ暗復号用暗号エンジンとを備えているのが好ましい。

【0024】

また、本発明が講じた解決手段は、コンテンツ再生方法として、外部メモリの再生不可領域に格納された原コンテンツをLSIに取り込むステップと、前記LSIにおいて、内部メモリに格納された固有IDを用いて、データ固有鍵を生成するステップと、前記LSIにおいて、前記原コンテンツを、前記データ固有鍵を用いて暗号化するステップと、暗号化されたコンテンツを、前記外部メモリの再生可能領域に格納するステップと、前記再生可能領域に格納された前記暗号化されたコンテンツを、前記LSIに取り込み、前記データ固有鍵を用いて復号化して再生するステップとを備えたものである。

【0025】

本発明によると、外部メモリの再生不可領域に格納された原コンテンツは、LSIにおいて、内部メモリに格納された固有IDを用いて生成されたデータ固有鍵を用いて、暗号化される。暗号化されたコンテンツは、外部メモリの再生可能

領域に格納され、再生のとき、データ固有鍵を用いて復号化される。このため、外部メモリの再生可能領域には、固有IDから生成されたデータ固有鍵を用いて暗号化されたコンテンツが格納されるので、同一のデータ固有鍵を有しない他のLSIによっては、再生が不能となる。このため、コンテンツの不正実行が防止され、セキュリティレベルが向上する。

【0026】

そして、前記本発明に係るコンテンツ再生方法において、前記原コンテンツは、データ共有鍵で暗号化されたものであり、前記原コンテンツを、前記データ固有鍵を用いて暗号化する前に、内部メモリに格納された前記データ共有鍵を用いて、復号化するのが好ましい。

【0027】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を参照して説明する。

【0028】

図1は本実施形態に係る半導体装置としてのセキュアLSIの内部構成を示すブロック図である。図1において、セキュアLSI1は外部バス120を介して、外部メモリ100（フラッシュメモリ101とRAM102）などと接続可能に構成されている。また、モードIDを与えることによって、その動作モードを設定することが可能になっている。

【0029】

本実施形態に関わる主な構成要素について、簡単に説明する。

【0030】

まず、セキュアLSI1は、書き換え不可領域11を含むセキュアメモリ（セキュアFlash）10を備えている。この書き換え不可領域11には、書き換え不可領域書き込みフラグ12が設けられている。書き換え不可領域書き込みフラグ12は、モードIDが一度セキュアメモリ10に書き込まれると、そのフラグ値が“可”から“済”になり、それ以降の書き換え不可領域11への書き込みを不能にする。なお、本実施形態では、セキュアメモリ10はフラッシュメモリによって構成されているが、もちろんこれに限定されるものではなく、不揮発性

のメモリであればどのようなものであってもかまわない。

【 0 0 3 1 】

また、暗号化部 2 はプログラムの暗号化や復号化を行うものであり、暗号化演算部としての秘密鍵演算処理部 2 0 と、暗号化制御部としての鍵生成・更新シーケンサ 3 0 と、プログラム暗号種を記憶する記憶部 3 5 とを備えている。秘密鍵演算処理部 2 0 は各種の鍵などを格納するレジスタを備えており、プログラムの暗号化処理または復号化処理を含む複数のシーケンスを実行可能である。鍵生成・更新シーケンサ 3 0 は秘密鍵演算処理部 2 0 が実行可能な各シーケンスについて実行の諾否を判断し、実行が許されないと判断したシーケンスについて秘密鍵演算処理部 2 0 の動作を禁止する。鍵生成・更新シーケンサ 3 0 はモード I D 格納レジスタ 3 1 を有しており、このモード I D 格納レジスタ 3 1 に格納されているモード I D の値に基づいて、各シーケンスの実行の諾否を判断する。また、鍵またはプログラムがどのようなアルゴリズムや鍵長で暗号化されているかを示す暗号種別識別子を格納する暗号種別識別子格納レジスタ 3 2 を備えている。暗号化部 2 の構成および動作の詳細については、後述する。

【 0 0 3 2 】

モードシーケンサ 4 0 も、モード I D 格納レジスタ 4 1 を備えており、モード I D 格納レジスタ 4 1 に格納されているモード I D と、ジャンパ 4 3 の値に応じて、外部インターフェース (I / F) 5 0 の動作、すなわち、外部メモリ 1 0 0 に格納されたプログラムやデータをどの I / F を介して読み込むか、が制御される。これにより、外部メモリ 1 0 0 に格納された平文プログラムが実行できるか否かを制御することができる。さらに、モードシーケンサ 4 0 は、鍵がどの手法によって暗号化されているかを示す暗号種別識別子を格納する暗号種別識別子格納レジスタ 4 2 を備えている。

【 0 0 3 3 】

外部 I / F 5 0 は、モードシーケンサ 4 0 の制御に従って、プログラム処理部 5 1 が有するスルー部 5 2 およびプログラム復号用暗号エンジン 5 3、並びに、データ処理部 5 5 が有するスルー部 5 6 およびデータ暗復号用暗号エンジン 5 8 のうちのいずれかを介して、外部メモリ 1 0 0 との間でプログラムやデータの入

出力を行う。

【0034】

ここで、後述するアドミニストレータモードとアプリプログラム開発を除いては、スルー部52を介して入力されたプログラムは、セキュアLSI1内部で実行されることはない。すなわち、スルー部52は、平文プログラムの暗号化、またはすでに暗号化されたプログラムを別の鍵を用いて再暗号化するときに有効とされるものであり、セキュアLSI1は、後述するアドミニストレータモードとアプリプログラム開発を除いては、スルー部52を介して入力されたプログラムへは動作を遷移しないように構成されている。したがって、例えば商品となったセキュアLSI1はスルー部52を介して平文プログラムを取り込んだとしても、これを実行することはできない。

【0035】

ブートROM60は、セキュアLSI1の起動動作を制御するブートプログラムを格納している。HASH演算部70は、セキュアLSI1に読み込まれたプログラムについてその正当性を検証するために、HASH値を演算する。

【0036】

また、外部メモリ100では、プログラムがフラッシュメモリ101に格納され、データ（コンテンツ）がRAM102に格納されている。外部ツール110には、セキュアLSI1の最初の起動時にセキュアメモリ10に格納する各種の初期値が格納されている。この初期値の種類は、設定される動作モードに応じて、異なったものになる。

【0037】

図2は図1のセキュアLSI1を用いた開発および製品化の全体の流れを表す図である。図2に示すように、セキュアLSI1は、アドミニストレータモード（モードID：00）、鍵生成モード（モードID：01）、開発モード（モードID：10）および商品動作モード（モードID：11）の4種類の動作モードで、動作する。

【0038】

まず、アドミニストレータモードに設定されたセキュアLSI1は、管理者用

L S I として、動作する。管理者用 L S I では、鍵生成プログラムが開発され（P A 1）、また、その鍵生成プログラムが任意の鍵生成鍵を用いて暗号化される（P A 2）。

【 0 0 3 9 】

鍵生成モードに設定されたセキュア L S I 1 は、鍵生成用 L S I として、動作する。鍵生成用 L S I では、管理者用 L S I において生成された、暗号化された鍵生成プログラムが実装され（P B 1）、この鍵生成プログラムを実行することによって、各種の鍵が生成される（P B 2）。

【 0 0 4 0 】

開発モードに設定されたセキュア L S I 1 は、開発用 L S I として、動作する。開発用 L S I では、実際の製品で実行されるアプリケーション用プログラムが開発される（P C 1）。そして、このアプリケーション用プログラムが、プログラム共有鍵を用いて暗号化される（P C 2）。

【 0 0 4 1 】

商品動作モードに設定されたセキュア L S I 1 は、実際の商品 L S I として、動作する。商品 L S I では、開発用 L S I において生成された、プログラム共有鍵で暗号化されたアプリケーション用プログラムが実装され、その内部で、プログラム固有鍵で暗号化されたアプリケーション用プログラムに、変換される（P D 1）。プログラム固有鍵で暗号化されたアプリケーションプログラムは通常の商品動作において実行される。なお、この変換処理は、開発用 L S I でも、アプリケーション用プログラムのデバッグ（P C 4）のために、実行可能になっている（P C 3）。

【 0 0 4 2 】

セキュア L S I 1 は、ブート ROM 6 0 に格納されたブートプログラムを実行することによって、以下のような動作を行う。

【 0 0 4 3 】

図 3 はブートプログラムの全体的な処理の流れを示すフローチャートである。セキュア L S I 1 に電源が投入されると、ブート ROM 6 0 に格納されたブートプログラムが CPU 6 5 によって実行される。図 3 に示すように、まず、各ハー

ドウェアを初期化する（SZ0）。そして、外部ツール110からさまざまな初期値を読み込み、セキュアメモリ10に設定する（SZ1）。

【0044】

図4は初期値設定処理SZ1のフローチャートである。まず、ジャンパ44で、セキュアメモリ10がLSI内に実装されているか否かの判定を行う（SZ11）。次に、書き換え不可領域書き込みフラグ12が“済”であるか否かを判定し（SZ12）、“済”であるときは（SZ12でYes）すでにセキュアメモリ10に初期値が設定されているので、処理SZ1を終了する。書き換え不可領域書き込みフラグ12が“可”であるときは（SZ12でNo）、セキュアメモリ10に初期値を書き込んでいく。モードIDに加えて、暗号化されたプログラム固有鍵、アドレス管理情報、データ固有鍵をセキュアメモリ10の書き換え不可領域11に書き込む（SZ13, SZ16～SZ18）。なお、最初の判定の結果、セキュアメモリ10がLSIの外部にあると判定されたとき（SZ14でNo）は、モードIDは商品動作モードを表す値に上書きされる（SZ15）。これにより、セキュアメモリ10がLSIパッケージ外にあるような製品は、商品動作モードでしか動作できない。

【0045】

次に、書き込み不可領域書き込みフラグ12を“済”にセットする（SZ19）。これによって、以後の書き換え不可領域11の書き換えはできなくなる。さらに、通常領域13, 14に暗号種別識別子および実装モードフラグを書き込む（SZ1A）。そして、モードIDがアドミニストレータモード以外のモードを示すときは（SZ1BでNo）、これらに加えて、暗号化された共有鍵／鍵生成鍵も通常領域13, 14に書き込む（SZ1C）。

【0046】

その後、図3にもどり、前処理SZ2を実行する。ここでは、セキュアメモリ10の書き込み不可領域11に設定されたモードIDが、鍵生成・更新シーケンサ30のモードID格納レジスタ31と、モードシーケンサ40のモードID格納レジスタ41とに設定される。また、セキュアメモリ10の第1の通常領域13に設定された暗号種別識別子が、鍵生成・更新シーケンサ30の暗号種別識別

子格納レジスタ 3 2 と、モードシーケンサ 4 0 の暗号種別識別子格納レジスタ 4 2 とに設定される。さらに、セキュアメモリ 1 0 の書き換え不可領域 1 1 に格納されたアドレス管理情報が、MEMC 8 0 のアドレス区分格納レジスタ 8 1 に設定される。ここまでの動作は、図 2 における初期値設定フェーズ P A 0, P B 0, P C 0, P D 0 に対応している。

【0 0 4 7】

その後は、モード I D の値に応じて、それぞれのモードにおける動作を行う（S Z 3）。

【0 0 4 8】

モード I D が「0 0」のとき、セキュア L S I 1 はアドミニストレータモードになり、ジャンパ 4 3 の値に応じて（S A 0）、平文プログラム実行処理 S A 1、またはプログラム暗号化処理 S A 2 を実行する。鍵生成プログラム開発フェーズ P A 1 では、平文プログラム実行処理 S A 1 が行われ、ここで、鍵生成プログラムが生成される。この鍵生成プログラムは外部メモリ 1 0 0 に格納される。鍵生成プログラム暗号化フェーズ P A 2 では、鍵生成プログラムを任意の鍵生成鍵で暗号化する。

【0 0 4 9】

モード I D が「0 1」のとき、セキュア L S I 1 は鍵生成モードになり、実装モードフラグの値に応じて（S B 0）、キージェネレータ製造処理 S B 1、または鍵管理・発行処理 S B 2 を実行する。キージェネレータ製造フェーズ P B 1 では、キージェネレータ製造処理 S B 1 が実行され、任意の鍵生成鍵で暗号化された鍵生成プログラムをプログラム固有鍵で再暗号化する。鍵管理・発行フェーズ P B 2 では、プログラム固有鍵で暗号化された鍵生成プログラムを実行させることによって、鍵管理・発行処理 S B 2 が実行し、鍵を生成する。

【0 0 5 0】

モード I D が「1 0」のとき、セキュア L S I 1 は開発モードになり、ジャンパ 4 3 の値に応じて（S C 0）、プログラム暗号化処理 S C 1、平文プログラム実行処理 S C 2、プログラム実装処理 S C 3、または暗号化プログラム実行処理 S C 4 を実行する。アプリケーションプログラム開発フェーズ P C 1 では、平文

プログラム実行処理 S C 2 が行われ、アプリケーションプログラムが開発される。開発されたアプリケーションプログラムは、外部メモリ 1 0 0 に格納される。アプリケーションプログラム暗号化フェーズ P C 2 では、プログラム暗号化処理 S C 1 が実行される。また、アプリケーションプログラム実装フェーズ P C 3 では、プログラム実装処理 S C 3 が実行され、アプリケーションプログラムデバッグフェーズ P C 4 では、暗号化プログラム実行処理 S C 4 が実行される。これらの処理は、商品動作モードにおける各処理 S D 1, S D 2 と同様である。

モード I D が「1 1」のとき、セキュア L S I 1 は商品動作モードになり、実装モードフラグの値に応じて (S D 0)、プログラム実装処理 S D 1、または通常ブート処理 S D 2 を実行する。商品実装フェーズ P D 1 では、プログラム実装処理 S D 1 が実行される。商品動作フェーズ P D 2 では、通常ブート処理 S D 2 が実行される。

【0 0 5 1】

図 5 は暗号化部 2 とその周辺の構成を示す図である。図 5 に示すように、鍵生成・更新シーケンサ 3 0 はモード I D 格納レジスタ 3 1 および暗号種別識別子格納レジスタ 3 2 の他に、秘密演算処理部 2 0 を用いて実行される各シーケンスに対応して設けられ、その発行回数を格納するためのレジスタ 3 3 と、レジスタ 3 1, 3 3 を参照して、各シーケンスを実行してよいか否か（ブート R O M 6 0 中の各プログラムおよび外部のプログラムを実行してよいか否か）を判断し、秘密鍵演算処理部 2 0 の動作を制御する制御部 3 4 とを備えている。セキュア L S I 1 において、各シーケンスが 1 回発行されると、これに対応したレジスタ 3 3 に 1 が加算される。

【0 0 5 2】

プログラム暗号種 3 5 は、鍵を復号するとき、または鍵を生成するときに用いられるものであり、共有鍵用と固有鍵用とがそれぞれ準備されている。

【0 0 5 3】

そして、上述の商品動作モードや開発モードにおいては、セキュアメモリ 1 0 に格納された値を暗号化部 2 の各レジスタに設定するシーケンス（セキュア F l a s h ロード）や鍵を生成・復号するシーケンス（鍵シーケンサ）はそれぞれ

1 回ずつしか発行できないように、制御部 3 4 によって制限がかけられる。例えば、セキュア L S I 1 の起動時に一度、ブートプログラムによってセキュアメモリに記憶されたモード I D がモード I D 格納レジスタ 3 1 に格納されると、二度とモード I D を書き換えることができない。また、セキュア L S I 起動時に共有鍵と固有鍵を復号し、秘密鍵演算処理部 2 0 内部のレジスタに格納すると、二度と鍵を生成・復号することはできない。したがって、外部メモリ 1 0 0 に鍵生成プログラムを実装したとしても、鍵は生成することはできない。一度復号された固有鍵は、外部 I / F 5 0 内の固有鍵格納レジスタに格納され、暗号化プログラムの実行はこの固有鍵を用いて行われる。また、プログラムの更新は、秘密鍵演算処理部 2 0 内部のレジスタに格納された共有鍵や固有鍵を用いて行われる。

【 0 0 5 4 】

なお、上述の鍵生成モードやアドミニストレータモードにおいては、鍵シーケンスに対する制限が外されるので、鍵を生成することができる。

【 0 0 5 5 】

ここで、シーケンス発行回数格納レジスタ 3 3 の代わりに、プログラム暗号種に対応して設けられ、その使用回数を格納するプログラム暗号種使用回数格納レジスタを設けてもよい。鍵を生成・復号するときにはプログラム暗号種が用いられるので、例えば、モード I D によってその使用回数を制限しておけば、プログラム暗号種の使用回数を計数することによっても、鍵の生成・復号を制限することができる。

【 0 0 5 6 】

また、プログラム暗号種は必ずしも共有鍵と固有鍵とをそれぞれ準備する必要はない。

【 0 0 5 7 】

図 6 はコモンバスとプライベートバスの設定方法を示す図である。ここで、「プライベートバス」とは、外部からのアクセス（外部アクセス）ができないバスのことをいい、外部 I / F 5 0 から必ずしも物理的に独立しているわけではない。すなわち、プライベートバス 9 1 につながっているとして設定されたレジスタ等は、外部アクセスでの読み出し・書き込みができない。

【 0 0 5 8 】

セキュア L S I 1 の内部のレジスタ等には、アドレスがそれぞれ与えられている。コモンバスアドレス格納部 8 2 はそのアドレスのうち、コモンバス 9 2 につながったレジスタ等のアドレス（図 6 では“0 X 0 0 0 0 0”～“0 X 1 0 0 0 0”）を記憶している。外部アクセスがあったときは、外部アクセスアドレス判定部 8 3 が、コモンバスアドレス格納部 8 2 を参照してコモンバス 9 2 へのアクセスか否かを判定し、そうであればこれを受け付ける。一方、外部アクセスがコモンバス 9 2 へのアクセスでないときは、プライベートバス 9 1 へのアクセスであるので、アクセスを拒否する。

【 0 0 5 9 】

なお、CPU 6 5 からのアクセス（内部アクセス）のときは、このような判定は行われず、内部アクセスは受け付けられる。

【 0 0 6 0 】

図 7 は外部 I / F 5 0 とその周辺の構成を示す図である。図 7 において、アドレス区分格納レジスタ 8 1 は、外部メモリ 1 0 0 における各領域と、アドレスとの対応関係を表すアドレス管理情報を格納している。ここでは、外部メモリ 1 0 0 を、第 1 の領域（設定範囲内のプログラム）、第 2 の領域（設定範囲外のプログラム）、第 3 の領域（設定範囲内のデータ）および第 4 の領域（設定範囲外のデータ）という 4 つの領域に分けて、そのアドレスを記憶している。

【 0 0 6 1 】

比較器 8 5 は、アドレス区分格納レジスタ 8 1 に格納されたアドレス管理情報を参照し、入出力しようとする情報のアドレスが上述の第 1 ～第 4 の領域のいずれに該当するかを判断し、その判断結果を入出力制御信号生成部 8 4 に送る。

【 0 0 6 2 】

入出力制御信号生成部 8 4 は、モードシーケンサ 4 0 から出力されたモード I D とジャンパ判定結果、および比較器 8 5 の出力に基づいて、外部 I / F 5 0 が有するどのインターフェースを有効にするかを判定し、その判定結果を入出力制御信号として外部入出力モード制御部 5 4 に送る。外部入出力モード制御部 5 4 は受けた入出力制御信号に従って、いずれかのインターフェースを有効にする。

なお、モード I D が商品動作モードを示すときは、実行スルー部 5 2 b は必ず有効にはしない。これにより、外部メモリ 1 0 0 に格納された平文プログラムは実行されないように制限される。

【 0 0 6 3 】

第 1 の領域に格納されたプログラムは、アドミニストレータモードや開発モードのデバッグ時は、プログラム処理部 5 1 の実行用スルー部 5 2 b を介して取り込まれ、鍵生成モード、商品動作モード、または開発モードでデバッグ時以外のときは、プログラム復号用暗号エンジン 5 3 を介して取り込まれる。これらのプログラムは実行可能である。一方、第 2 の領域に格納されたプログラムは、プログラム処理部 5 1 の暗号化用スルー部 5 2 a を介して取り込まれ、暗号化部 2 に供給され、暗号化または再暗号化される。これらのプログラムは実行不可能である。

【 0 0 6 4 】

また、第 3 の領域に格納されたデータは、データ処理部 5 5 のデータ暗復号用暗号エンジン 5 8 を介して取り込まれ、第 4 の領域に格納されたデータは、データ処理部 5 5 のスルー部 5 6 を介して取り込まれる。

【 0 0 6 5 】

暗号化用スルー部 5 2 a を介して取り込まれたプログラムは、暗号化部 2 の秘密鍵演算処理部 2 0 において暗号化または再暗号化された後、再び暗号化スルー部 5 2 a を介して、外部メモリ 1 0 0 の第 1 の領域に書き込まれる。これにより、以降は実行可能なプログラムとなる。

【 0 0 6 6 】

なお、アドレス区分格納レジスタ 8 1 およびモード I D 格納レジスタ 4 1 は、プライベートバス 9 1 を介して、データが設定される。すなわち、内部からのアクセスによってデータ設定がなされる。また、このデータ設定は、セキュア L S I 1 のリセット後、1 回のみ実行可能である。

【 0 0 6 7 】

図 8 は外部 I / F 5 0 の動作を示す図であり、商品動作モードを想定している。図 8 に示すとおり、実装前には、共有鍵で暗号化されたアプリケーションプロ

グラムが外部メモリ 1 0 0 の第 2 の領域（設定範囲外）に格納されており、このため、このままでは実行することができない。すなわち、第 2 の領域に格納された、共有鍵で暗号化されたアプリケーションプログラムは、実装時に暗号化用スルー部 5 2 a を介してセキュア L S I 1 内部に取り込まれ、共有鍵で復号化された後、固有鍵で再暗号化され、再び暗号化用スルー部 5 2 a を介して、外部メモリ 1 0 0 の第 1 の領域（設定範囲内）に格納される。そして、この第 1 の領域に格納された、固有鍵で暗号化されたアプリケーションプログラムは、プログラム復号用暗号エンジン 5 3 を介してセキュア L S I 1 内部に取り込まれ、実行される。

【 0 0 6 8 】

なお、開発モードでは、次のような動作を行う。まずデバッグ時には、実行したいプログラムを第 1 の領域（設定範囲内）に書き込んでおく。これにより、平文プログラムであっても、実行用スルー部 5 2 b を介して取り込まれ、実行される。暗号化時には、暗号化したいプログラムを第 2 の領域（設定範囲外）に書き込んでおく。これにより、セキュア L S I 1 を起動すると、暗号化シーケンスが実行され、共有鍵で暗号化されて外部メモリ 1 0 0 に格納される。デバッグ実装時には、再暗号化したいプログラムを第 2 の領域（設定範囲外）に書き込んでおく。さらには、暗号化デバッグ時には、デバッグしたい暗号化プログラムを第 1 の領域（設定範囲内）に書き込んでおく。これにより、復号されて実行される。

【 0 0 6 9 】

図 9 はセキュアメモリ 1 0 のアクセス制御を示す図である。図 9 に示すように、アクセス制御部 9 5 は、書き換え不可領域 1 1 のアドレスを格納するレジスタ 9 6 と、書き換え不可領域書き込みフラグ 1 2 のアドレスを記憶するレジスタ 9 7 と、書き込み可／不可判定部 9 8 とを備えている。レジスタ 9 6、9 7 は、データが一度書き込まれると、フラグ管理などによって、さらなる書き込みができないように構成されている。

【 0 0 7 0 】

アクセス制御は、次のように行われる。CPU 6 5 からセキュアメモリ 1 0 へのアクセスは、必ず、アクセス制御部 9 5 を介して実行される。コマンドが「リ

ード」のときは、アクセス先のアドレスが、書き換え不可領域または通常領域のいずれであっても、セキュアメモリ 1 0 のデータはプライベートバス 9 1 に出力される。一方、コマンドが「ライト」のときは、書き込み可／不可判定部 9 8 が、アクセス先のアドレスとレジスタ 9 6 に格納されたアドレス、および書き換え不可領域書き込みフラグ 1 2 の値を参照して、書き込みを行うか否かを判定する。具体的には、次のような判断を行う。

(フラグ“済”	かつ	書き込み不可領域)	…	書き込み不可
(フラグ“済”	かつ	通常領域)	…	書き込み可
(フラグ“未”	かつ	書き込み不可領域)	…	書き込み可
(フラグ“未”	かつ	通常領域)	…	書き込み可

【0 0 7 1】

なお、セキュアメモリ 1 0 には、「セクタ消去」や「チップ消去」などのコマンドも準備されている。書き換え不可領域書き込みフラグ 1 2 が“済”のとき、「セクタ消去」は通常領域については受け付けるが、書き込み不可領域については受け付けない。また「チップ消去」は受け付けない。

【0 0 7 2】

また、コンテンツ（データ）の再生においても、次のような方法を採用することによって、セキュリティを向上させている。

【0 0 7 3】

データは当初、外部 RAM 1 0 2 における第 4 の領域（設定範囲外）に置かれている。第 4 の領域に置かれているとき、データは、データ共有鍵（プログラム共有鍵と異なる）によって暗号化された状態か、または平文の状態である。このため、他の L S I によって不正利用される可能性があり、セキュリティの面で問題がある。

【0 0 7 4】

この問題を解決するために、不正利用を特に防止したい映像や音楽等のコンテンツについては、コンテンツを再生するプログラムを、外部 RAM 1 0 2 の第 3 の領域（設定範囲内）に記憶されたコンテンツしか再生できないように作成する。第 3 の領域内に置かれたデータは、セキュア L S I に取り込まれるとき、デー

タ暗復号用暗号エンジン 5 8 において復号化される。この復号化において用いられるデータ固有鍵は、固有 I D と乱数によって作成されるので、セキュア L S I 1 毎に異なるだけでなく、起動毎にも異なっている。したがって、データは不正利用されにくくなり、セキュリティが向上する。なお、コンテンツを再生するプログラムも固有鍵で暗号化されているので、改竄されにくいと考えられる。

【 0 0 7 5 】

図 1 0 および図 1 1 は商品動作モードにおける通常ブート処理のデータフローである。図 1 0 において、まず、セキュアメモリ 1 0 の書き込み不可領域 1 1 に格納されている、暗号化されたプログラム固有鍵 E n c (プログラム固有鍵、M K 0) , E n c (M K 0, C K) を秘密鍵演算処理部 2 0 の暗号鍵格納レジスタに設定する。そして、この暗号化されたプログラム固有鍵を、実装されたプログラム暗号種を用いて復号し、プログラム固有鍵を得る。得たプログラム固有鍵は、外部 I / F 5 0 のプログラム復号用暗号エンジン 5 3 のプログラム固有鍵格納レジスタに設定する。その後、セキュアメモリ 1 0 の書き込み不可領域 1 1 に格納されているデータ固有 I D を秘密鍵演算処理部 2 0 の固有 I D 格納レジスタに設定する。また、C P U 6 5 によって乱数を生成し、秘密鍵演算処理部 2 0 の乱数格納レジスタに設定する。そして、秘密鍵演算処理部 2 0 によって、データ固有 I D と乱数からデータ固有鍵を生成する。生成されたデータ固有鍵は、外部 I / F 5 0 のデータ暗復号用暗号エンジン 5 8 のデータ固有鍵格納レジスタに設定される。

【 0 0 7 6 】

その後、図 1 1 において、外部メモリ 1 0 0 に格納されていた、プログラム固有鍵で暗号化されたアプリケーションプログラム E n c (アプリケーションプログラム、プログラム固有鍵) を、外部 I / F 5 0 が有するプログラム処理部 5 1 のプログラム復号用暗号エンジン 5 4 を介して復号し、H A S H 演算部 7 0 に取り込み、H A S H 値を演算する。そして、この演算した H A S H 値と、セキュアメモリ 1 0 の通常領域 1 3 に格納されていた H A S H 値とを比較し、アプリケーションプログラムが改ざんされていないかどうかをチェックする。H A S H 値が一致していたとき、外部メモリ 1 0 0 に格納されていたアプリケーションプログ

ラム E n c（アプリケーションプログラム、プログラム固有鍵）に処理を遷移し、アプリケーションを実行する。なお、H A S H 値が一致していないときは、何らかの不正が行われたものと推定して、不正アクセス時制御による処理を実行する。

【 0 0 7 7 】

アプリケーションプログラムは、CPU 6 5 によって実行される。すなわち、セキュア L S I 1 内部の CPU 6 5 がマスターとなってアクセス制御を行うので、以降の動作は内部アクセスとなり、したがって、外部アクセスアドレス判定部 8 3 は関与しない。アプリケーションプログラムによって、外部 R A M 1 0 2 の第 4 の領域（再生不可領域）から、データ共有鍵で暗号化されたコンテンツ（原コンテンツ）がセキュア L S I 1 に取り込まれる。取り込まれたコンテンツは、セキュアメモリ 1 0 に書き込まれたデータ共有鍵を用いて、秘密鍵演算処理部 2 0 において復号化される。その後、外部 I / F 5 0 のデータ処理部 5 5 におけるデータ暗復号用暗号エンジン 5 8 を介してデータ固有鍵で暗号化され、外部 R A M 1 0 2 の第 3 の領域（再生可能領域）に書き込まれる。以降、このデータ固有鍵で暗号化されたコンテンツは再生可能となり、再生されるとき、外部 I / F 5 0 のデータ処理部 5 5 におけるデータ暗復号用暗号エンジン 5 8 を介して、データ固有鍵で復号化される。

【 0 0 7 8 】

【発明の効果】

以上のように本発明によると、実行が許されると暗号化制御部によって判断されたシーケンスのみが、暗号化演算部によって実行される。このため、シーケンスの不正実行を未然に防止することができる。また外部インターフェースにおいて、プログラム処理部とデータ処理部とが別個独立に構成されている。このため、プログラムが不正実行されるリスクが分散される。さらに、外部メモリの再生可能領域には、固有 I D から生成されたデータ固有鍵を用いて暗号化されたコンテンツが格納されるので、同一のデータ固有鍵を有しない他の L S I によっては再生が不能となる。このため、コンテンツの不正実行が防止される。したがって、セキュリティレベルが向上する。

【図面の簡単な説明】

【図 1】

本発明の実施形態に係る半導体装置としてのセキュア L S I の構成を示すブロック図である。

【図 2】

図 1 のセキュア L S I を用いた開発および製品化の全体の流れを表す図である。

【図 3】

ブートプログラムの全体的な処理の流れを示すフローチャートである。

【図 4】

初期値設定処理 S Z 1 のフローチャートである。

【図 5】

図 1 のセキュア L S I における暗号化部とその周辺の構成を示す図である。

【図 6】

図 1 のセキュア L S I におけるコモンバスとプライベートバスの設定方法を示す図である。

【図 7】

図 1 のセキュア L S I における外部ホスト I / F とその周辺の構成を示す図である。

【図 8】

商品動作モードにおける外部ホスト I / F の動作を示す図である。

【図 9】

セキュアメモリのアクセス制御を示す図である。

【図 1 0】

商品動作モードにおける通常ブート処理のデータフローその 1 である。

【図 1 1】

商品動作モードにおける通常ブート処理のデータフローその 2 である。

【符号の説明】

- 1 セキュア L S I (半導体装置)

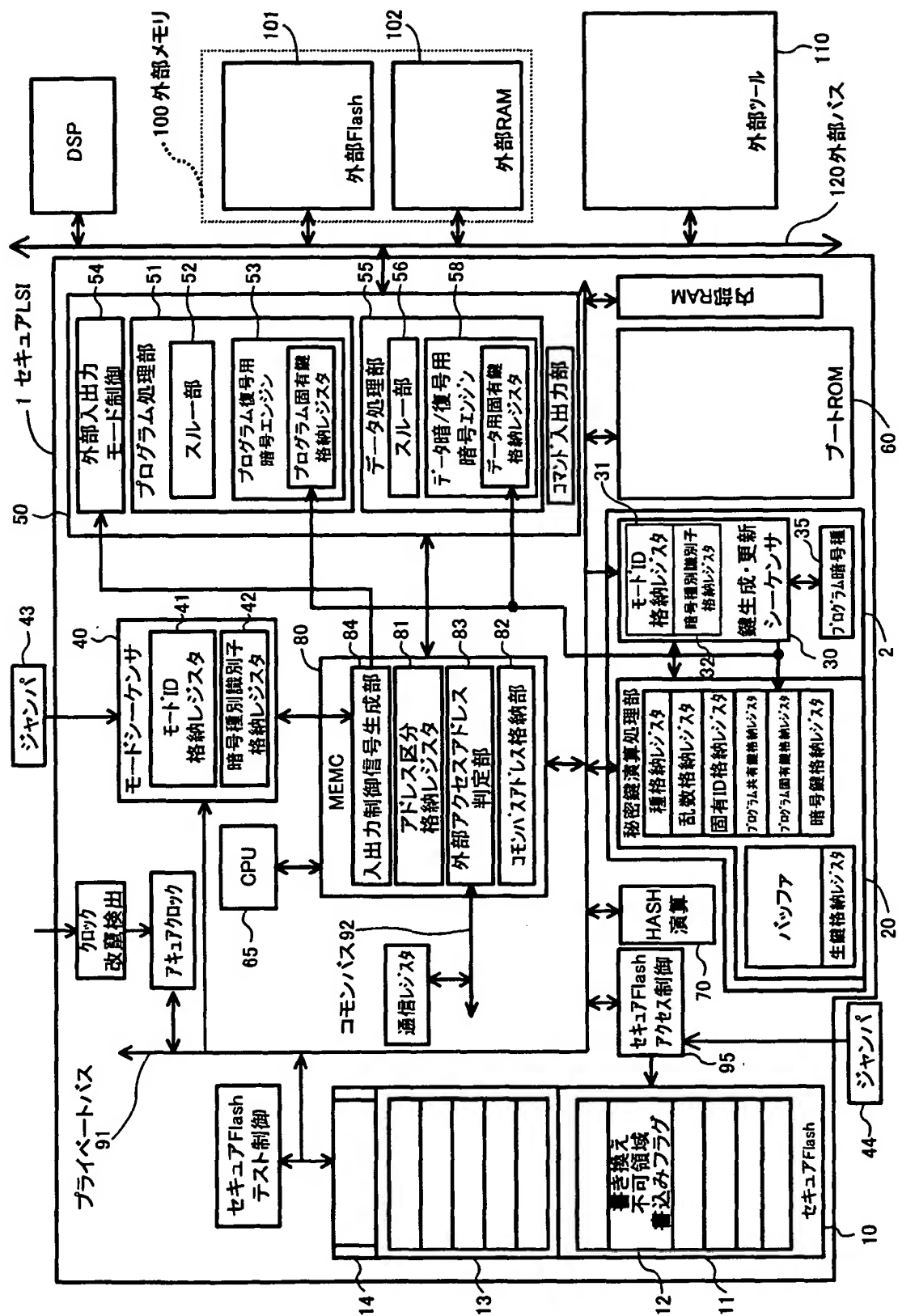
2 暗号化部

- 1 0 セキュアメモリ
- 1 1 書き換え不可領域
- 2 0 秘密鍵演算処理部（暗号化演算部）
- 3 0 鍵生成・更新シーケンサ（暗号化制御部）
- 3 1 モード I D 格納レジスタ
- 3 3 シーケンス発行回数格納レジスタ
- 3 5 記憶部
- 4 0 モードシーケンサ
- 4 1 モード I D 格納レジスタ
- 4 5 ジャンパ値判定部
- 5 0 外部インターフェース
- 5 1 プログラム処理部
- 5 2 スルー部
 - 5 2 a 実行用スルー部
 - 5 2 b 暗号化用スルー部
- 5 3 プログラム復号用暗号エンジン
- 5 5 データ処理部
- 5 6 スルー部
- 5 8 データ暗復号用暗号エンジン
- 6 0 ブート R O M
- 8 1 アドレス区分格納レジスタ
- 8 2 コモンバスアドレス格納部
- 8 3 外部アクセスアドレス判定部
- 1 0 0 外部メモリ

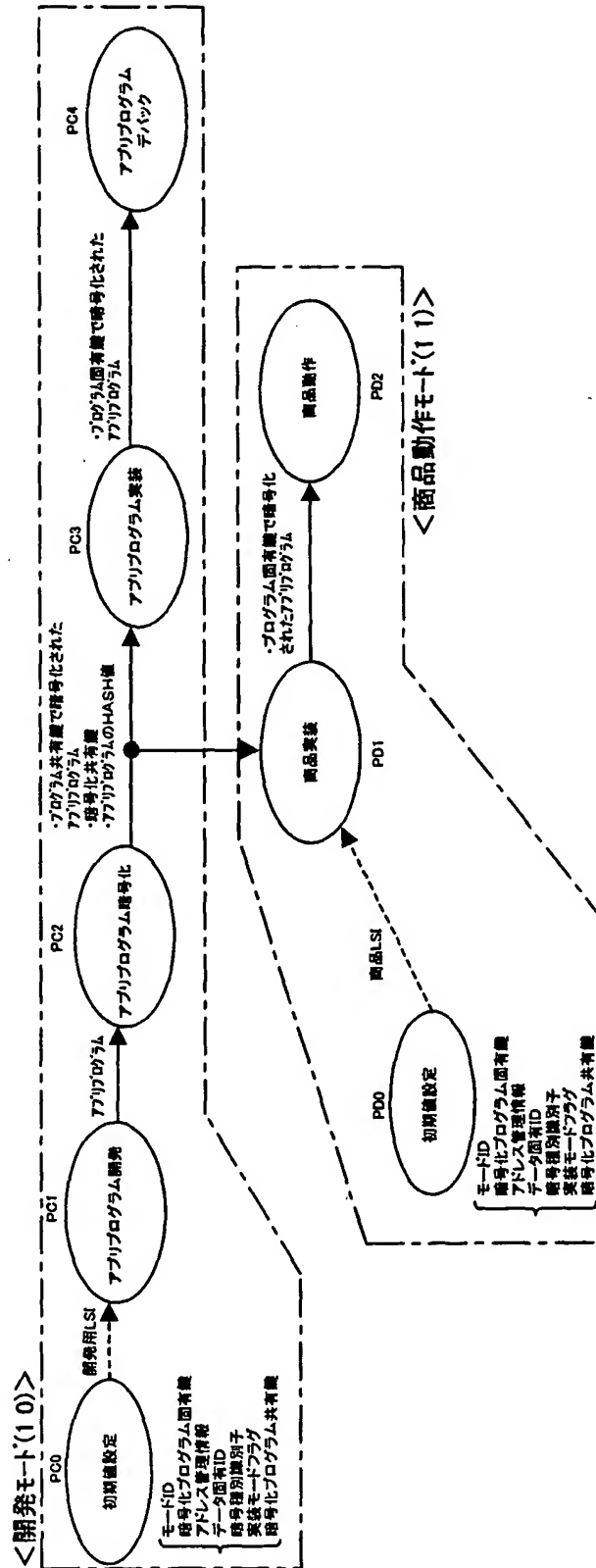
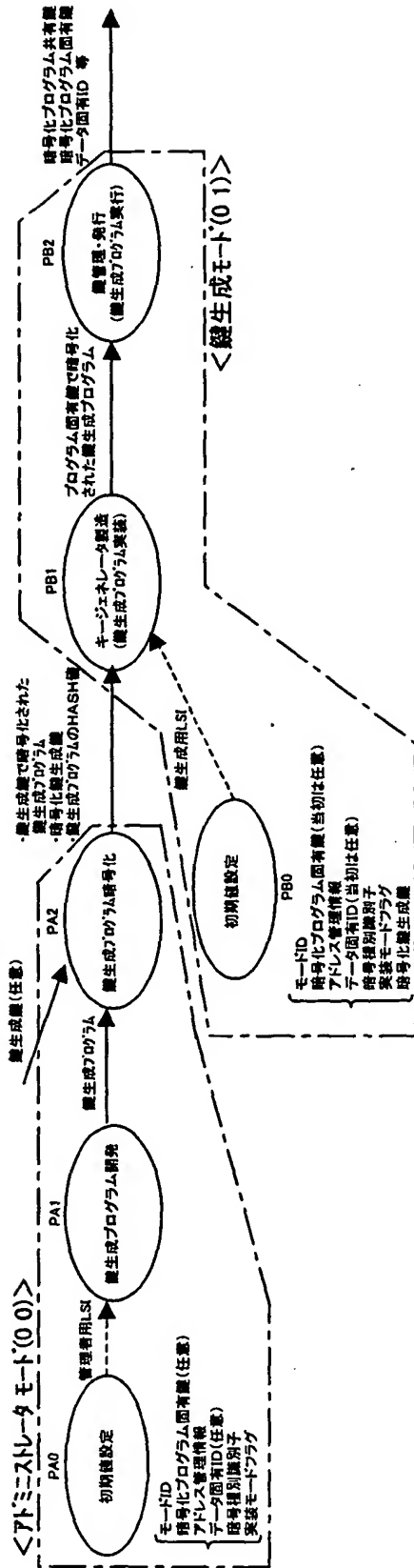
【書類名】

凶面

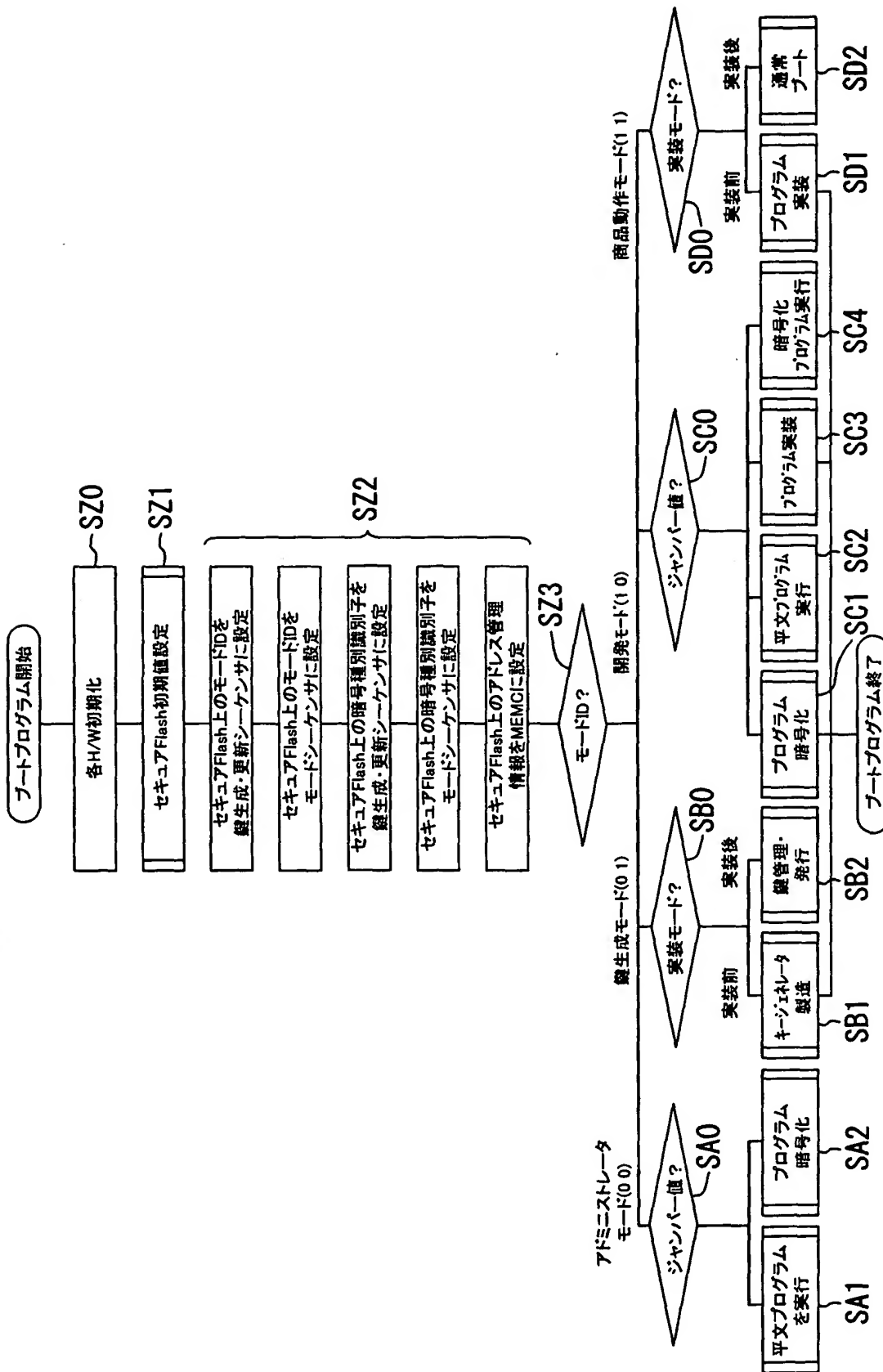
【図 1】



【図 2】

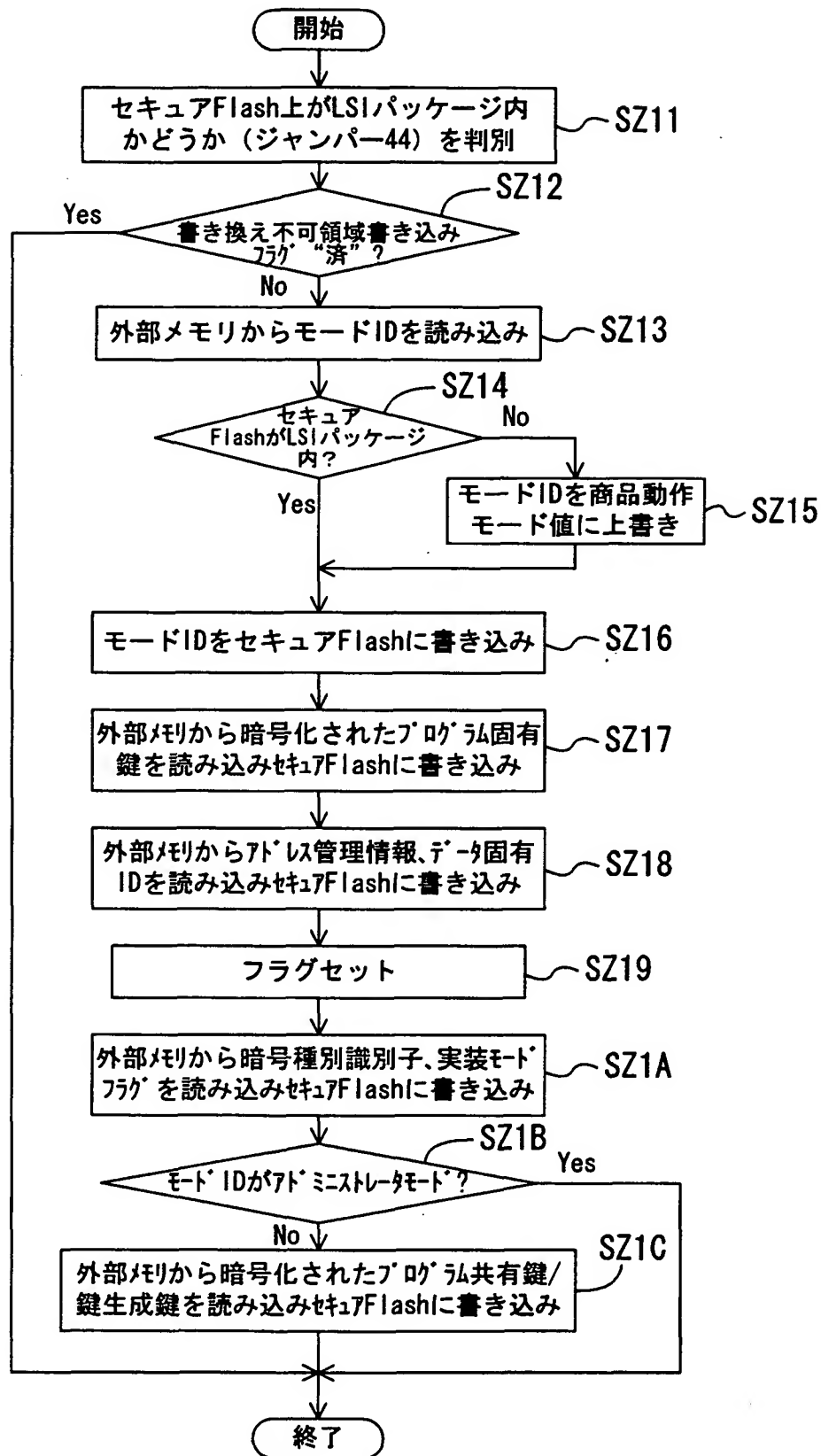


【図 3】

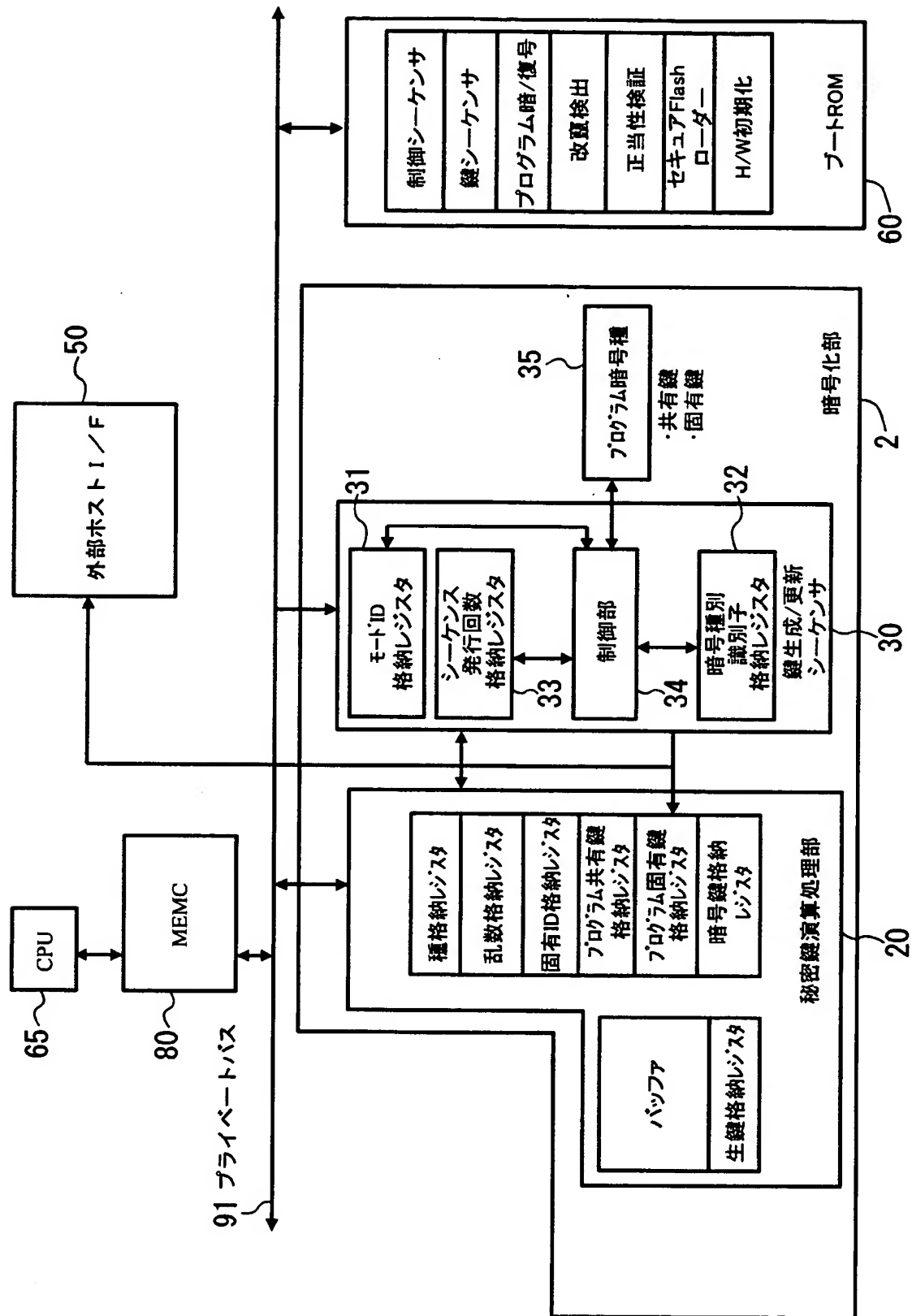


【図4】

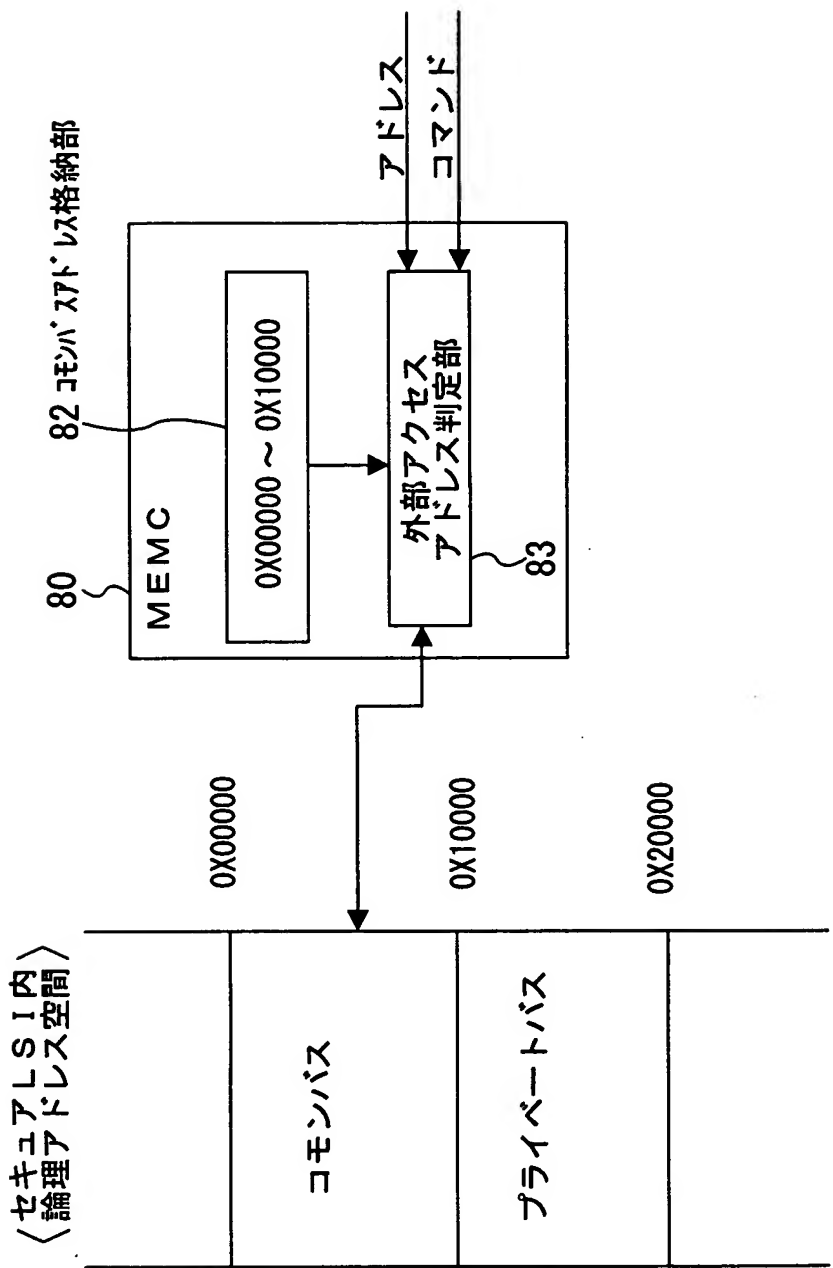
SZ1



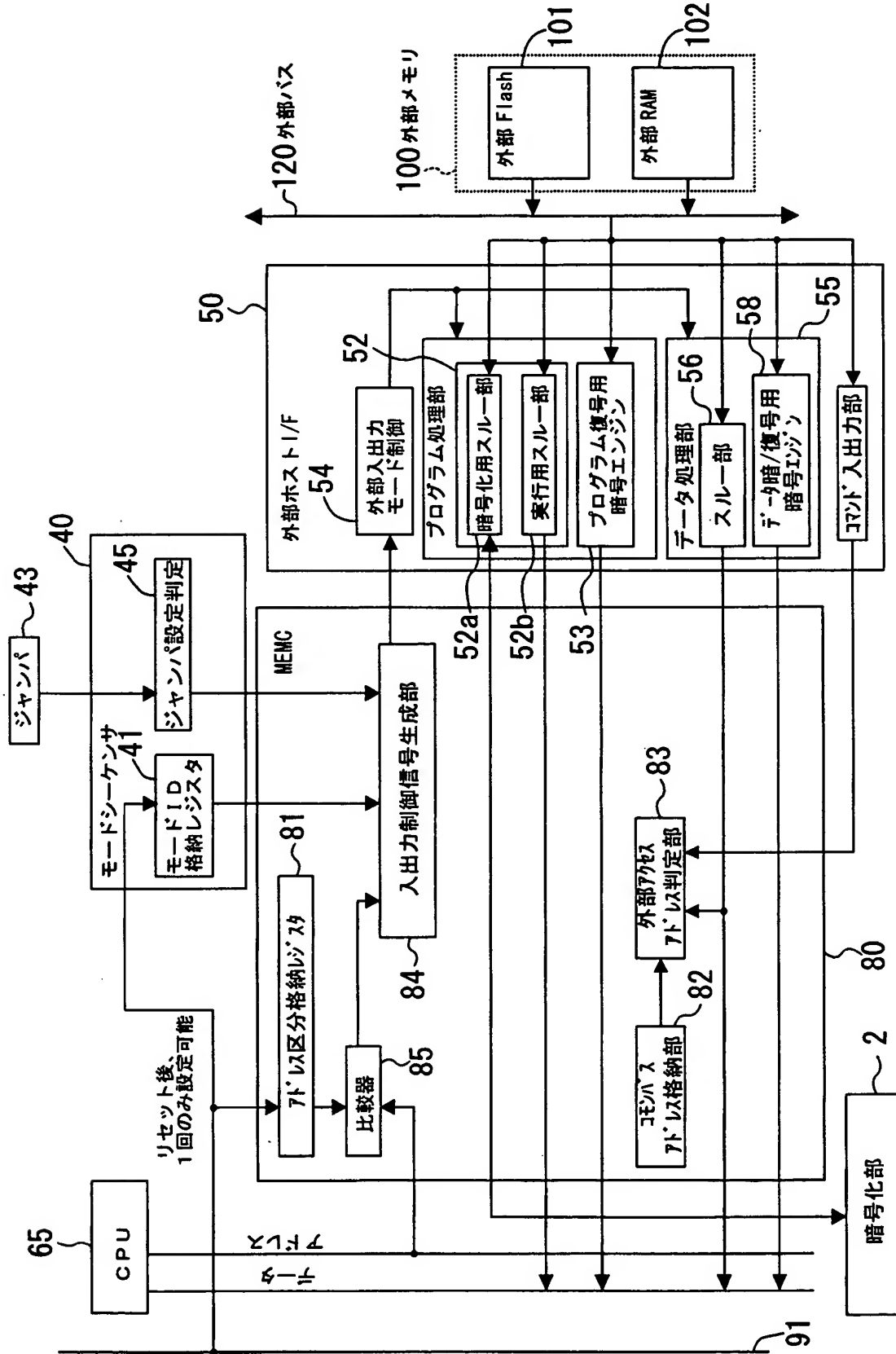
【図5】



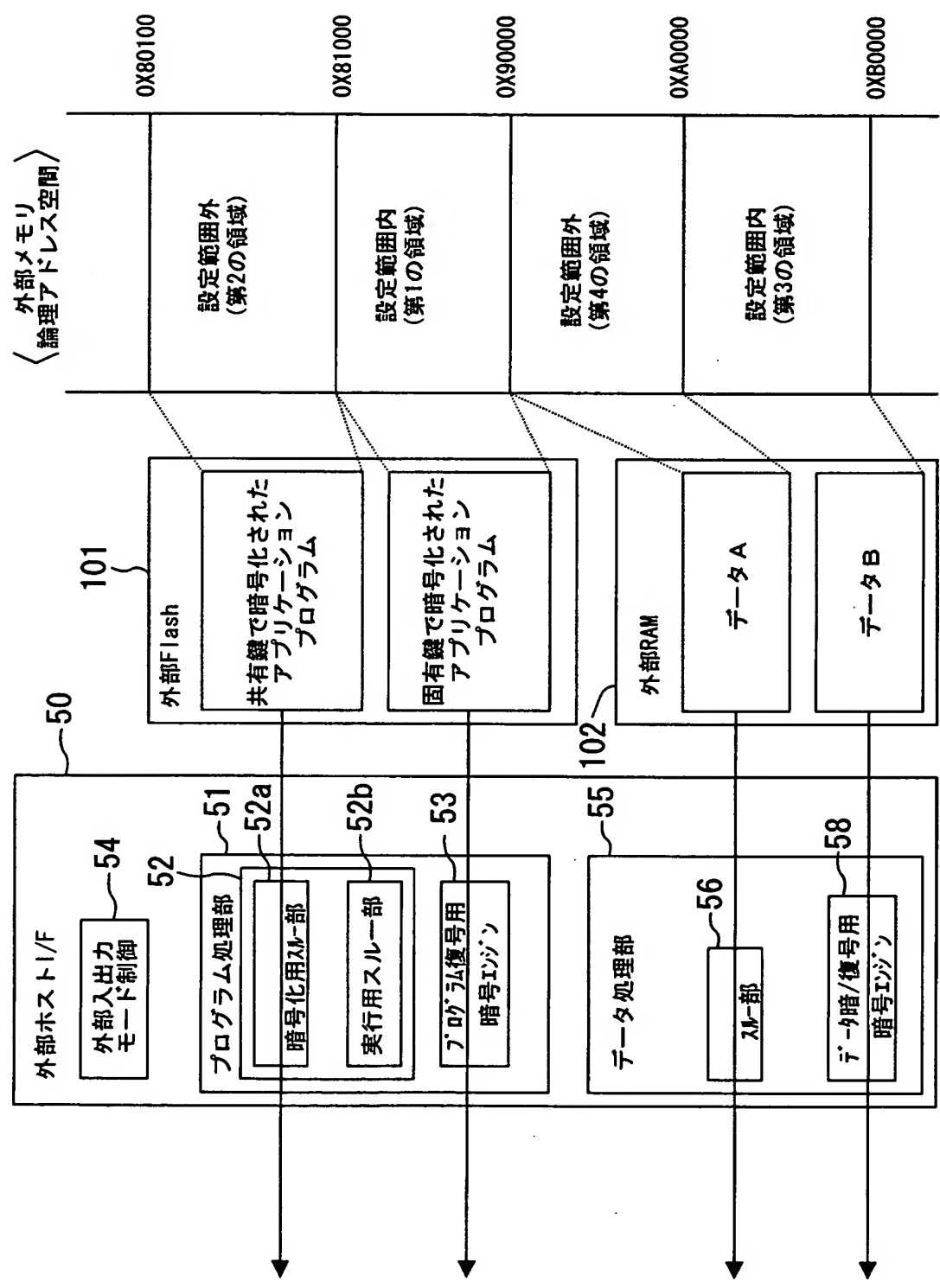
【図 6】



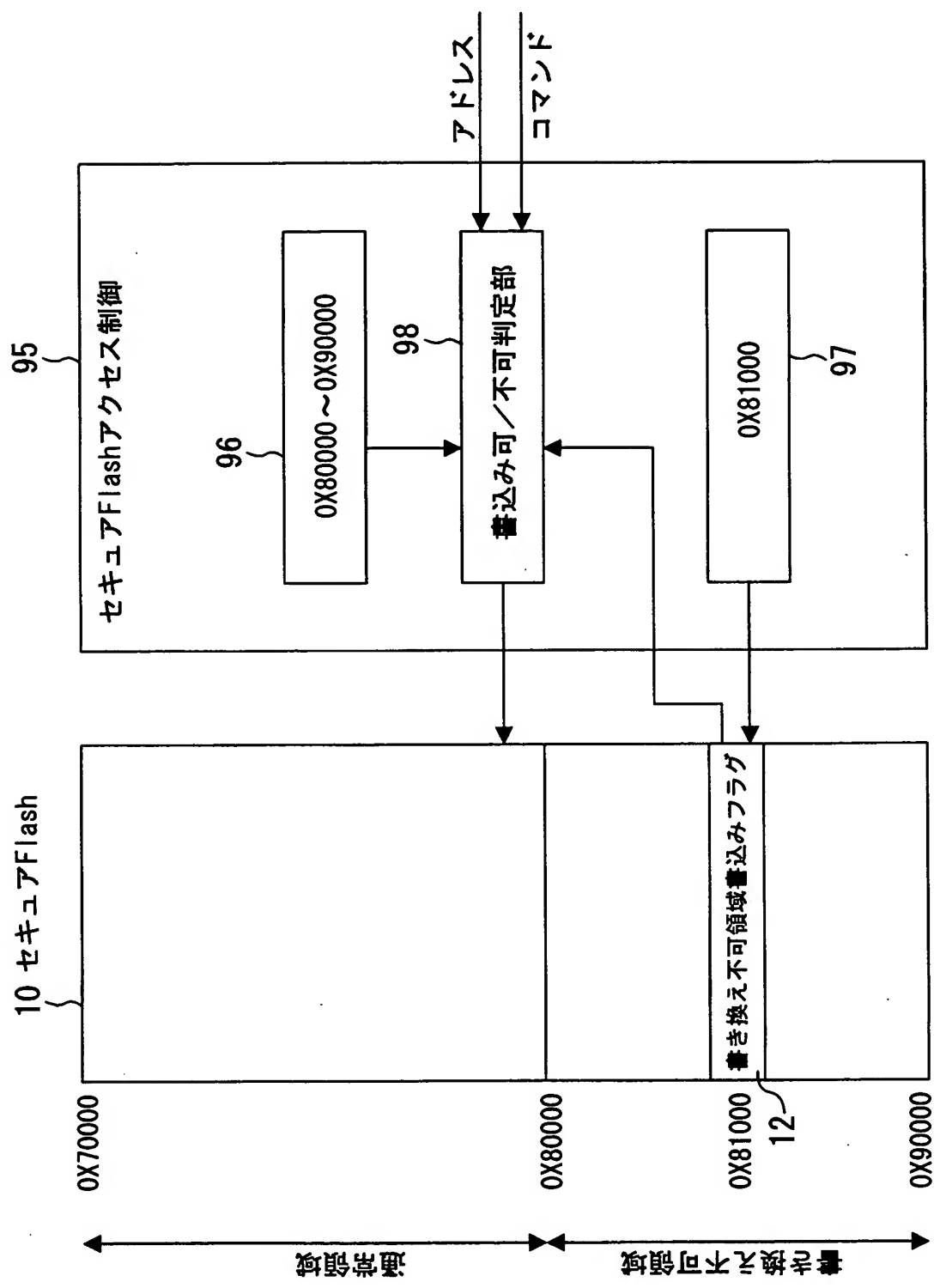
【図7】



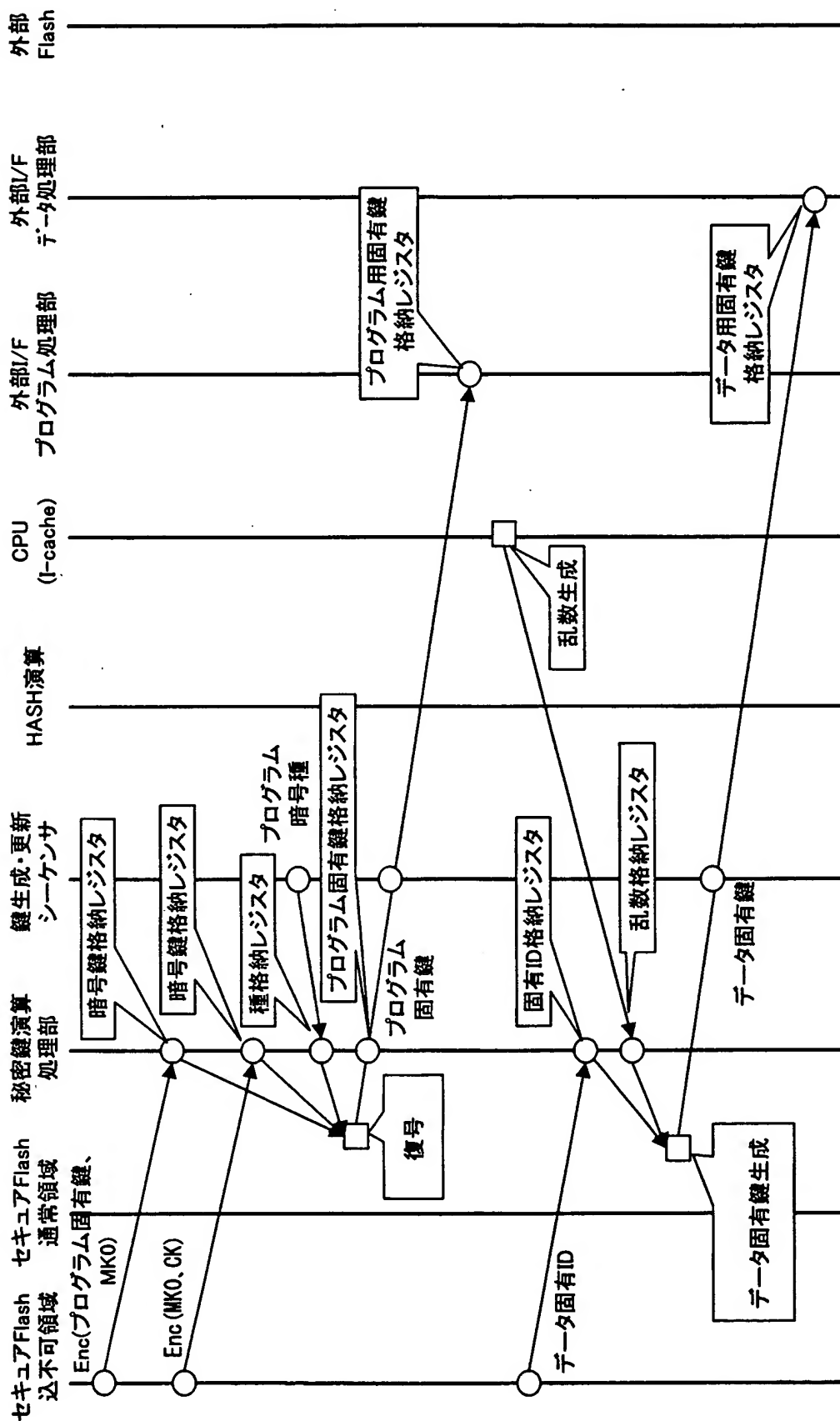
【図 8】



【図9】



【図10】



【書類名】 要約書

【要約】

【課題】 セキュリティレベルの高い半導体装置を提供する。

【解決手段】 セキュア L S I 1 は、プログラムの暗号化を行う暗号化部 2 と、外部メモリ 1 0 0 との間でプログラムやデータの入出力を行うための外部 I / F 5 0 とを備えている。暗号化部 2 において、鍵生成・更新シーケンサ 3 0 が、実行が許されないと判断したシーケンスについて、秘密鍵演算処理部 2 0 の動作を禁止する。外部 I / F 5 0 では、プログラム処理部 5 1 とデータ処理部 5 5 とが別個独立に構成されている。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住 所 大阪府門真市大字門真1006番地

氏 名 松下電器産業株式会社